WHITEPAPER

Protect patient privacy to maintain patient trust

imprivata®

Patient care is the core principle for all healthcare organizations. That's nothing new. But increasingly, that principle goes far beyond the physical health of patients and extends to digital health. That means that protecting patient privacy is as critical as providing the best care.

A patient's clinical care team is still their care team, but a new, less obvious expansion is happening behind the scenes, too. With patient privacy playing such a critical role in overall safety and experience, IT, compliance, and privacy teams are the care team's newest – and increasingly important – members. And with an ever-expanding field of digital identities at play – of both patients and care providers alike – everyone has a role to play:

- **Clinicians |** Ensure patients are cared for effectively
- **IT teams |** Empower clinicians to deliver high-quality care without roadblocks while protecting the organization from risk
- **Compliance and privacy teams |** Protect highly sensitive patient data from risk

While compliance and privacy teams are directly responsible for ensuring the privacy of data, truly protecting patient data is everyone's job. Especially when patient trust is on the line.

But there are so many things that can make executing on the principle – *the promise* – of patient privacy easier said than done. Internal and external threats are rising, and valuable patient data is often the target. And managing appropriate access to patient data isn't always as buttoned up as you'd like.

But ensuring patient privacy is a requirement you can't afford to ignore. Reputational damage, financial loss, and fines and penalties for regulation noncompliance is nothing to scoff at (with minimum HIPAA violation fines of $50,000![1]) – but what's most at stake is patient trust.

The elephants in the room: What's getting in the way of protecting patient privacy, and earning patient trust

If protecting patient privacy is such an obvious requirement for healthcare organizations, why are we still talking about it?

Well, it's not that simple.

But with 47% of customer churn impacted by the relationship with the organization, and their trust that their privacy is protected[2], it's critical to know – and overcome – any blockers.

THE TROUBLE WITH MANUAL PROCESSES

So many organizations are still relying on manual processes for patient privacy protection. And while manual processes are of course better than no processes, they present many opportunities for things to slip through the cracks. Often, the choice to stick with manual processes has everything to do with budgets and teams that only seem to be getting more restricted.

Organizations with fully deployed security AI and automation save an average of $3.05 million when breaches occur.

But remember: healthcare organizations have massive amounts of data coming through their doors every day – and manually parsing through all of it, including log files and access rights, is not just time-consuming, but nearing on impossible. Even with multiple people assigned to data review tasks. And it's certainly not scalable.

For comprehensive patient privacy protection schemes to be successful, solutions need to be able to scale. Manual processes are simply too time-consuming and labor intensive to reach any true level of efficacy. Especially when that's compounded across the many teams who are responsible for patient privacy. (Reminder: every team!)

And when organizations with fully deployed security AI and automation save an average of $3.05 million when breaches occur than those without[3], there's really no reason to lean on manual processes.

STARTING FROM THE BEGINNING WITH PATIENT IDENTIFICATION

To paraphrase an adage, when inaccurate or incomplete data comes in, the overall data profile is unlikely to get any more "hygienic" as the data travels. It's easier to protect data when everyone who interacts with it can confidently expect it to be accurate and complete. And that whole process starts at intake, with ensuring patients are who they say they are, and positively connecting them to their existing data. This may sound obvious, but a staggering 10% of patients are misidentified during medical record searches, and, of misidentification events, 9% led to patient harm[4].

When patients can be confident that the data following them around is, in fact, their data, their trust in the organization providing them appropriate care increases. And when clinicians can be confident about that same thing, patient health outcomes improve.

There's no hiding that there are some roadblocks to effectively protecting patient privacy, but there are ways forward. And everyone has the ability to make a difference.

It's easier to protect data when everyone who interacts with it can confidently expect it to be accurate and complete.

The key to patient privacy protection: Automated solutions

Patient privacy is everyone's job, and while departments don't have to be (or often need to be) on the same page, they all need to at least be reading the same book to ensure nothing gets missed. And one way to get everyone aligned is to ditch those manual processes in favor of automated – and purpose-built – solutions.

Automated solutions can help:

- Detect, and investigate, insider threats to PHI
- Ensure appropriate access protocols are put in place, keeping data safe, with the help of provisioning and deprovisioning
- Audit internal access to patient data
- Positively identity patients at any point of care
- Increase patient trust and satisfaction

With trusted, automated solutions in place, everyone responsible for ensuring that patient privacy is protected can be confident that nothing will fall through the cracks.

MANAGE ACCESS RIGHTS

It's not just external threats you need to worry about. Internal threats – malicious or not – put patient data at risk. That's why every effort needs to be made to ensure appropriate access rights. Workflows need to be considered, of course, but to protect patient data and privacy, access should only be granted when truly necessary. With automated provisioning and deprovisioning, and visibility into access events and permissions, an identity governance solution helps all departments feel confident about their patient privacy practices.

ENSURE POSITIVE PATIENT IDENTIFICATION

The better – and more complete – data is at the beginning, the more likely it can be protected. Ensuring that patients are linked to their unique medical record improves patient safety and reduces medical errors, increasing trust in the process and in the organization. And clinicians can be confident that they're working with the right, complete patient data.

MONITOR FOR PATIENT PRIVACY BREACHES

Being able to quickly uncover inappropriate access to patient data is a critical part of protecting patient privacy. Even with preventative measures in place, malicious intent can find a way. But with a patient privacy monitoring solution, clinicians, IT teams, and compliance and privacy teams can be confident that any breaches won't go unnoticed. And patients can be confident, too.

When patient privacy is everyone's job, leaning on automated, and trusted, solutions can be the key to ensuring patient trust.

GET A JUMPSTART ON PROTECTING PATIENT PRIVACY >

[1] https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

[2] https://security.imprivata.com/trust-in-depth-the-comprehensive-approach-to-data-privacy-wp.html?chnl=ImpEmWeb

[3] https://www.ibm.com/reports/data-breach?utmcontent=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjw67ajBhAVEiwA2g_jED2tPMmkFsrt1yN9c-s8Mwsbj4lBrrZ23riRWAc2hlwloV8MSv1rLhoCsFMQAvD_BwE&gclsrc=aw.ds

[4] Wall Street Journal Healthcare Report, Should Every Patient Have a Unique ID Number for All Medical Records, July 2012. Valenstein, P. N., Raab, S. S. & Walsh, M. K. Identification errors involving clinical laboratories: a College of American Pathologists Q-Probes study of patient and specimen identification errors at 120 institutions. Arch. Pathol. Lab. Med. 130, 1106–1113 (2006)

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow,security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform ofinteroperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage andsecure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com